LISTING OF CLAIMS

This listing of claims below will replace all prior versions and listings of claims in the present application.

1. (Currently amended) A method for validating a public key certificate by a computer in a public key infrastructure composed of a plurality of certificate authorities including an end entity certificate issuing authority, wherein:

the end entity certificate issuing authority issues to an end entity a public key certificate used for validating a signature generated by an end entity apparatus operated by the end entity,

the method comprises:

a path registration step of registering in a database a valid path extending from a certificate authority being a start certificate authority to any end entity certificate issuing authority, and

a certificate validation step of receiving a certificate validation request for a public key certificate issued by any end entity certificate issuing authority, judging the validity of the public key certificate of which the certificate validation has been requested using information registered in the database, and outputting a result of the judgment,

the path registration step and the certificate validation step are executed by the computer independently of one another,

the path registration step comprises the following steps executed by the computer:

step 1) searching a path extending from the start certificate authority to the end entity certificate issuing authority which is the end of the path;

step 2) validating the path searched in step 1; and

step 3) registering the path which has been validated in step 2 as a valid path in the database, and

the certificate validation step comprises the following steps executed by the computer:

step 4) checking whether there is registered in the database a path specified by the request for certificate validation, the path extending from the start certificate authority being the trust anchor of an originator of the request for certificate validation to the end entity certificate issuing authority which has issued the public certificate of which the certificate validation has been requested, and which is the end of the path,

step 5) if the checked path is registered in the database as the valid path in step 4, validating a signature of the public key certificate of which the certificate validation is requested, by using the public key certificate issued to the end entity certificate issuing authority being the end of the checked path, and if validation of the signature is successful, judging that the public key certificate of which the certificate validation has been requested is valid and outputting a result of the judgment;

step 6) if the checked path is not registered in the database as the valid path in step 4, searching a path that includes a partial path from the start certificate authority being the trust anchor to the end entity certificate issuing authority which has issued the public key certificate of which certificate validation is requested and which is the end of the path, and that extends from the start certificate authority being the trust anchor to the end entity which is an issue destination of the public key certificate of which certificate validation is requested;

step 7) in the searching step in step 6, if the path extending from the start certificate authority being the trust anchor to the end entity being the issue destination of the public key certificate of which certificate validation is requested is detected, validating the path that includes the partial path and extends from the start certificate authority being the trust

anchor to the end entity being the issue destination of the public key certificate of which certificate validation is requested;

step 8) judging the validity of the public key certificate of which certificate validation is requested based on the validation result in step 7 and outputting a result of the judgment; and

step 9) registering the partial path included in the path validated in step 7 into the database as a valid path.

2. (Previously presented) A method according to claim 1, further comprising step 10 executed by the computer, in which

if the specified path is not detected in step 6 of the certificate validation step, judging that the public key certificate of which certificate validation is requested is not valid, and outputting the result of the judgment.

3. (Previously presented) The method of claim 1, further comprising the following steps executed by the computer:

step 11) validating a revocation list issued by the end entity certificate issuing authority as to the public key certificate issued by the end entity certificate issuing authority in step 2 by using the public key certificate issued to the end entity certificate issuing authority;

step 12) if the validation in step 11 is successful, registering the revocation list as a valid revocation list in the database, in association with the valid path to be registered in step 3;

step 13) as the public key certificate issued by the end entity certificate issuing authority which is the end of the partial path in step 7, validating the revocation list issued by the end

entity certificate issuing authority by using the public key certificate issued to the end entity certificate issuing authority;

step 14) if the validation in step 13 is successful, registering the revocation list as a valid revocation list in the database in association with the partial path to be registered in the database in step 9.

4. (Previously presented) The method of claim 3, further comprising the following steps executed by the computer:

step 15) checking in step 5, whether the public key certificate of which the certificate validation is requested is invalid or not, using the valid revocation list which has been registered in association with the checked path; and

step 16) if the signature validation in step 5 is successful and the public key certificate of which the validation is requested is valid in step 15, judging that the public key certificate of which certificate validation is requested is valid, and if the signature validation is failed, or the public key certificate of which the validation is requested is invalid, judging that the public key certificate of which certificate validation is requested is not valid.

5. (Previously presented) The method of claim 1, further comprising step 17 executed by the computer, in which:

if the path checked in step 4 of the certificate validation step is registered as the valid path in the database, checking in step 5 whether the public key certificate of which the certificate validation is requested or any other public key certificates issued by other certificate authorities included in the checked path includes any constraint item;

if the path includes any constraint item, checking whether the checked path observes the constraint; and

if the path observes the constraint, judging that the public key certificate of which the certificate validation is requested is valid.

6. (Previously presented) The method of claim 1, further comprising step 18 executed by the computer, in which:

if the path checked in the step 4 of the certificate validation step is registered in the database as the valid path, checking in step 5, whether the certificate validation request includes any policy and checking whether the public key certificate of which the certificate validation is requested or other public key certificates issued by any other certificate authorities included in the checked path satisfies the policy included in the certificate validation request; and

if the public key certificate of which the certificate validation is requested or other public key certificates satisfies the policy, judging that the public key certificate of which the certificate validation is requested is valid.

7. (Previously presented) A method for validating validity of a public key certificate as defined in claim 6, wherein:

in a case where, at the validity validation step, the path corresponding to the validity validation request is registered as the valid path in the database, it is validated without validating the certificate revocation list that the pertinent public key certificate is not revoked.

8. (Currently amended) A computer program product comprising at least one computer readable storage medium bearing instructions, said instructions, when executed, being

arranged to cause at least one processor to perform steps for validating a public key certificate by a computer in a public key infrastructure composed of a plurality of certificate authorities including an end entity certificate issuing authority, the steps comprising:

registering in a database a valid path extending from a certificate authority being a start certificate authority to any end entity certificate issuing authority,

receiving a certificate validation request for a public key certificate issued by any end entity certificate issuing authority,

judging the validity of the public key certificate of which the certificate validation has been requested using information registered in the database, and

outputting a result of the judgment, wherein:

the path registration step and the step of judging certificate validity are executed by the computer independently of one another, [[and]]

the path registration step comprises:

step 1) searching a path extending from the start certificate authority to the end entity certificate issuing authority which is the end of the path;

step 2) validating the path searched in step 1; and

step 3) registering the path which has been validated in step 2 as a valid path in the database, and

the step of judging certificate validity comprises:

step 4) checking whether there is registered in the database a path specified by the request for certificate validation, the path extending from the start certificate authority being the trust anchor of an originator of the request for certificate validation to the end entity certificate issuing authority which has issued the public certificate of which the certificate validation has been requested, and which is the end of the path,

step 5) if the checked path is registered in the database as the valid path in step 4, validating a signature of the public key certificate of which the certificate validation is requested, by using the public key certificate issued to the end entity certificate issuing authority being the end of the checked path, and if validation of the signature is successful, judging that the public key certificate of which the certificate validation has been requested is valid and outputting a result of the judgment;

step 6) if the checked path is not registered in the database as the valid path in step 4, searching a path that includes a partial path from the start certificate authority being the trust anchor to the end entity certificate issuing authority which has issued the public key certificate of which certificate validation is requested and which is the end of the path, and that extends from the start certificate authority being the trust anchor to the end entity which is an issue destination of the public key certificate of which certificate validation is requested;

step 7) in the searching step in step 6, if the path extending from the start certificate authority being the trust anchor to the end entity being the issue destination of the public key certificate of which certificate validation is requested is detected, validating the path that includes the partial path and extends from the start certificate authority being the trust anchor to the end entity being the issue destination of the public key certificate of which certificate validation is requested;

step 8) judging the validity of the public key certificate of which certificate validation is requested based on the validation result in step 7 and outputting a result of the judgment; and

step 9) registering the partial path included in the path validated in step 7 into the database as a valid path.

9. (Previously presented) A product according to claim 8, further comprising step 10 executed by the computer, in which

if the specified path is not detected in step 6 of the certificate validation step, judging that the public key certificate of which certificate validation is requested is not valid, and outputting the result of the judgment.

10. (Previously presented) The computer readable medium of claim 8, further comprising the following steps executed by the computer:

step 11) validating a revocation list issued by the end entity certificate issuing authority as to the public key certificated issued by the end entity certificate issuing authority in step 2 by using the public key certificate issued to the end entity certificate issuing authority;

step 12) if the validation key certificate in step 11 is successful, registering the revocation list as a valid revocation list in the database, in association with the valid path to be registered in step 3;

step 13) as the public key certificate issued by the end entity certificate issuing authority which is the end of the partial path in step 7, validating the revocation list issued by the end entity certificate issuing authority by using the public key certificate issued to the end entity certificate issuing authority;

step 14) if the validation in step 13 is successful, registering the revocation list as a valid revocation list in the database in association with the partial path to be registered in the database in step 9.

11. (Previously presented) The computer readable medium of claim 10, further comprising the following steps executed by the computer:

step 15) checking in step 5, whether the public key certificate of which the certificate validation is requested is invalid or not, using the valid revocation list which has been registered in association with the checked path; and

step 16) if the signature validation in step 5 is successful and the public key certificate of which the validation is requested is valid in step 15, judging that the public key certificate of which certificate validation is requested is valid, and if the signature validation is failed, or the public key certificate of which the validation is requested is invalid, judging that the public key certificate of which certificate validation is requested is not valid.

12. (Previously presented) The product of claim 10, further comprising step 17 executed by the computer, in which:

if the path checked in step 4 of the certificate validation step is registered as the valid path in the database, checking in step 5 whether the public key certificate of which the certificate validation is requested or any other public key certificates issued by other certificate authorities included in the checked path includes any constraint item;

if the path includes any constraint item, checking whether the checked path observes the constraint; and

if the path observes the constraint, judging that the public key certificate of which the certificate validation is requested is valid.

13. (Previously presented) The product of claim 10, further comprising step 18 executed by the computer, in which:

if the path checked in the step 4 of the certificate validation step is registered in the database as the valid path, checking in step 5, whether the certificate validation request includes

any policy and checking whether the public key certificate of which the certificate validation is requested or other public key certificates issued by any other certificate authorities included in the checked path satisfies the policy included in the certificate validation request; and

if the public key certificate of which the certificate validation is requested or other public key certificates satisfies the policy, judging that the public key certificate of which the certificate validation is requested is valid.

14. (Previously presented) A product as defined in claim 13, wherein:

in a case where, at the validity validation step, the path corresponding to the validity validation request is registered as the valid path in the database, it is validated without validating the certificate revocation list that the pertinent public key certificate is not revoked.